Login : Jurnal Teknologi Komputer
ISSN : 2302-9692 (print) | 2723-8695 (online)
Vol. 13, No. 2, December 2019, pp. 24-28
LOGIN http://login.seaninstitute.org/index.php/Login

Implementation of Data Based Record Security using The Luc Method

Sakaria Efrata Ginting[1], Hery Sunandar[2], Zekson Arizona Matondang[3]
[1]Information Systems Study Program, Sekolah Tinggi Ilmu Komputer Medan, Indonesia,
[2]Faculty of Computer Science, Universitas Budi Darma, Medan, Indonesia,
[3]Informatics Engineering Study Program, STMIK Kristen Neumann, Medan, Indonesia.

Article Info

Article history:

Received, Okt 11, 2019
Revised, Nov 10, 2019
Accepted, Des 15, 2019

Keywords:

Implementation,
Database Record,
Security,
Luc method.

ABSTRACT

Cryptography is defined as the study of how to hide messages so that they cannot be read by those who are not blessed. Security in cryptography has become a very important aspect of an information system. Security problems often get less attention from designers and processors. Cryptography applications can be used to secure data. Therefore, database record users need help to meet the security needs of data stored in a Database Record or database. Records are the contents or data of managed tables that are interrelated and various data are stored in the table and cannot be manipulated. One of the safest methods for the above purposes is to use the Luc safety technique. Luc is a public cryptographic algorithm that uses a set of prime numbers to generate public and private keys. In this research, we will try to implement a mathematical science called cryptography. With the existence of cryptography which includes the encryption and decryption process, messages, data, and information can be coded so that unauthorized people cannot read the information and return it to its original state, other than people who do not know the key to decrypt it.

Corresponding Author:

Sakaria Efrata Ginting,
Information Systems Study Program,
Sekolah Tinggi Ilmu Komputer Medan,
Jl. Jamin Ginting No.285, Kwala Bekala, Kec. Medan Johor, Kota Medan, Sumatera Utara 20131.
Email: sakariaginting1983@gmail.com

1. INTRODUCTION

Security is one of the most important aspects of an information system. Security problems often get less attention from designers and processors. To secure the confidentiality of information or data, in order to avoid computer crimes committed by unauthorized people, one way to do this is by utilizing cryptographic techniques, especially in securing databases. Cryptography can be used to secure data.

Record is a collection of related data elements in a database. In summary, a database can be said to be a table that has row alias records and columns or fields. Each row represents related data elements[1].

Many types of cryptographic algorithms to secure secret messages. One of the algorithms used in securing message data is using the LUC algorithm, this algorithm uses two keys, namely the public key (for encryption) and the secret key (for decryption). Operations on LUC are carried out in the numeric domain, therefore before encryption, the text is converted into numeric. The LUC

algorithm uses the Lucas function where the value of the Lucas sequence up to n terms is very fast, so the modulo function N> 2 is developed.

2. RESEARCH METHOD

The stages in this research are described in the form of a diagram in order to understand each stage carried out. The stages of this research can be seen in Figure 1 below:

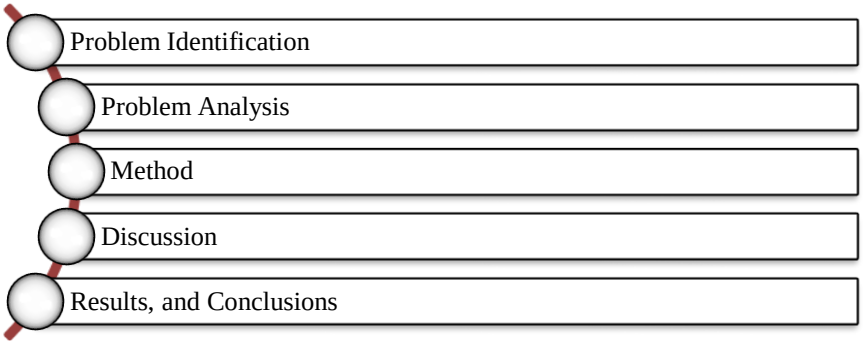

Figure 1. Diagram of Methods and Research Stages

2.1. Basic theory

A. North West Corner

Luc's algorithm is a cryptographic method using two different keys. The increase in the value of the Lucas sequence to n terms is very fast, so the function modulo N> 2 is developed. So that it satisfies the equation: V_n (P mod N, Q mod N) = V_n (P, Q) mod N If Q = 1 then we get the function: V_n (P, 1) mod N. So that the Lucas function that will be used in the Luc algorithm is:

V_{de} (P, 1) ≡ P mod N

Ve (M mod N, 1) ≡ C, where C is ciphertext Then the ciphertext is decrypted with the other Lucas sequences, namely: Vd (C mod N, 1) ≡ M Where n is e or d, some of the functions above aim to speed up n iteration calculations. In the development of the Lucas sequence as an algorithm in cryptography, only the Lucas Vn (P, Q) function will be used[2]

B. LUC algorithm

In the LUC algorithm, there are three main parts, namely the key generator, the encryption process, and the decryption process[3].

1. Key Generation

   In the LUC algorithm, when generating a key pair requires two prime numbers p and q.

   a. Choose any two prime numbers, for example, p and q where p ≠ q.
   b. Calculate the value of N = p x q.
   c. Count all numbers that are relatively prime to (p-1), (p + 1), (q-1) and (q + 1).
   d. Choose one of the random numbers from the results obtained in point (3) as the public key e.
   e. D = m2-4, where m is the plaintext to be encrypted.
   f. Look for the Legendre symbol from $\frac{D}{P}$ and $\frac{D}{q}$
   g. S(N)=LCM $\left[\left(p-\left(\frac{D}{p}\right)\right).\left(q-\left(\frac{D}{q}\right)\right)\right]$
   h. Hitung *ed* = 1 mod S(N) nilai (d,N) merupakan dekripsi (kunci privat) pasangan dari (e,n) Nilai *d* diperoleh dengan cara berikut : *e.d* = 1 mod S (N)

$$d = \frac{1 + k.S(N)}{e}$$

C. LUC Encryption Algorithm

Plaintext m will be encrypted with the public key e obtained from the key generator. Each block that has been obtained (mi) is converted into ASCII form then encrypted with the equation ci = Ve (mi, 1) mod N.[4]

D. LUC Decryption Algorithm

The decryption process of a ciphertext is almost the same as the process of encrypting a message, the difference is that the equation used is mi = Vd (ci, 1) mod N[5].

3. RESULTS AND DISCUSSION

Problem analysis aims to describe and resolve problems that exist in the system where the application is built. In the analysis phase of database record security can be done by:

1. LUC algorithm key generator

   Choose two prime numbers namely p and q but p ≠ q

   a. Calculate the value of N = p x q = 47 x 233 = 10951.
   b. Count all numbers that are prime relative to (p-1), (p + 1), (q-1) and (q + 1) to determine the value of e.
      Relative Prime = (p-1) = (46) = {3,5,7,11,13,17,… .., 43}
      Relative Prime = (p + 1) = (47) = {3,5,7,11,13,17,19,…., 47}
      Relative Prime = (q-1) = (232) = {7,11,13,17,19,23,29,31,37,41,43, ……., 229}
      Relative Prime = (p + 1) = (233) = {3,5,7,13,17,19,23,29,31,37,41,43, .., 233}
   c. From these calculations there are several numbers that are the same, namely {7,13,17,19,29,31,37,41,43,47} the value of e is chosen from these numbers, for example e = 46 then the public key is (e, N) = (10951).
   d. Calculate D = m2-4 where m is the plaintext to be encrypted. d = (7382) 2-4 legender symbols for
      $\frac{D}{P}$ is $\frac{54493920}{19}$ = -1, while the Legendre symbol for $\frac{D}{q}$ is $\frac{54493920}{19}$ =1
      The next step is to find LCM $\left(p-\frac{D}{p}, q-\frac{D}{q}\right)$
      S(n) =LCM(p+1,q-1)
      S(n) =LCM(47+1,233-1) =232

      Note that d e = 1 (mod n) so e.d = $\frac{1+k.s(n)}{e}$ with this formula, the value is obtained
      d = $\frac{1+(19.233)}{43}$ d = 103
      then you get the private key is (103, 10951).

2. The encryption process

   Is the process of securing information and the information cannot be read without the help of special knowledge or encryption can be defined[6]. If the last character does not have a partner, then add a space character using the Lucas $C_i = V_e (m_i, 1) \bmod N$. In the security process in the LUC method, the following steps can be taken:

   a. Determine the public key (e) and modulus (n) with the value of e = 43 and the value of n = 10951.
   b. Then break the plaintext (m) into blocks m_1, m_2, ... Table name "HERY SUNANDAR ". When separated into blocks, it will change to "HE", "RY", "SU", "N", "AN", "DA", "R"
      738265878284738373826582
      m1=7382 m2=6587 m3=8284 m4=7332 m5=8373 m6=8269 m7=7165 m8=8232

   Using the public key generated in the previous step (e, N) = (43, 10951), find the Lucas Chain sequence in k [x].

Table 1. Determination of the Lucas Chain

X	k[x]	e
1	1	e- 1 = 43
2	0	e/ 2 = 21
3	1	e- 1 = 20

4	0	e/ 2 = 10
5	1	e- 2 = 5
6	0	e/ 1 = 4
7	1	e- 2 = 2
8	0	e/ 2 = 1

It is found k [x] = {1,0,1,0,1,0,1,0} where k [x] is the laser chain, so k [x] = {0,1,0,1,0,1, 0.1}. To get the results of encryption calculations, the formula c_i = Ve (m, 1) mod N is used, then the results can be calculated in the table below.

Table 2. Name encryption calculation results

k[x]	v_n	hasil
0	v_2	3818
1	v_4	4446
0	v_5	8567
1	v_{10}	7614
0	v_{20}	4495
1	v_{21}	6702
0	v_{42}	5300
1	v_{43}	3544

3. The decryption process The process for converting ciphertext into plaintext For the first block to be decrypted using the private key that has been generated (103, 10951), the decryption process is carried out using the decryption equation V_d (C_i mod N, 1) = M.

Table 3. Lucas Chain Determination

X	k[x]	d
1	1	d-1 = 102
2	0	d/2 = 51
3	1	d-1 = 50
4	0	d/2=25
5	1	d-1 = 24
6	0	d/2 = 12
7	0	d/2 = 6
8	0	d/2 = 3
9	1	d-1 = 2
10	0	d/2 = 1

The results of the decryption calculation can be seen in the following table:

Table 4. Name decryption calculation results

k[x]	v_n	Hasil
1	v_2	7626
0	v_3	9760
1	v_6	3805
0	v_{12}	1856
1	v_{24}	7400
0	v_{25}	9784
0	v_{50}	7356
0	v_{51}	2822
1	v_{102}	3154
0	v_{103}	7382

4. CONCLUSION

The conclusions that the authors obtained from this study are: For the process of encryption and decryption of database records using the LUC method, while the plaintext is broken into blocks containing 2 characters, the process of securing database records using the LUC method with encryption and decryption algorithms. The use of Visual Basic 2008 programming language in designing an encryption and decryption application by implementing the LUC algorithm in the application can be made quite well.

REFERENCES

[1] J. B. Rahman, Muhsin, and Y. Nurhayati, "IMPELEMENTASI ALGORITMA LUC UNTUK PENGAMANAN PESAN BERBASIS ANDROID," *J. NUANSA Inform.*, vol. 12, no. 1, pp. 37–43, 2018.
[2] W. Y. S. Prasetya, M. Abdurohman, and D. W. Sudiharto, "ANALISIS DAN IMPLEMENTASI LUC UNTUK PENYANDIAN DATA MULTIMEDIA," *Fak. Tek. Inform. Telkom Univ.*, 2012.
[3] D. Ramadani, "Implementasi Algoritma LUC Dalam Penyandian Teks," *MEANS (Media Inf. Anal. dan Sist.*, vol. 3, no. 1, pp. 36–41, 2018.
[4] L. Renyta and I. Puteri, "ANALISIS DAN IMPLEMENTASI ALGORITMA KRIPTOGRAFI KUNCI PUBLIK RSA DAN LUC UNTUK PENYANDIAN DATA," *J. Ilm. DASI*, vol. 16, no. 3, pp. 27–36, 2015.
[5] R. Munir, *Kripografi*. Bandung: Informatika, 2006.
[6] R. Sadikin, *Kriptografi Untuk Keamanan Jaringan Dan Implementasi Dalam Bahsa Java*. Yoyakarta: ANDI Yogyakarta, 2012.